

(19)日本国特許庁 (J P)

(12) 公開特許公報 (A)

(11)特許出願公開番号

特開平9-204361

(43)公開日 平成9年(1997)8月5日

(51)Int.Cl. ⁸	識別記号	庁内整理番号	F I	技術表示箇所
G 0 6 F 12/14	3 2 0		G 0 6 F 12/14	3 2 0 C
	15/00	3 3 0		3 3 0 G
G 0 6 K 17/00			G 0 6 K 17/00	E
				F
G 0 9 C 1/00	6 6 0	7259-5 J	G 0 9 C 1/00	6 6 0 A
審査請求 未請求 請求項の数 8 O L (全 16 頁) 最終頁に続く				

(21)出願番号 特願平8-11899

(22)出願日 平成8年(1996)1月26日

(71)出願人 000006013

三菱電機株式会社

東京都千代田区丸の内二丁目2番3号

(71)出願人 391024515

三菱電機セミコンダクタソフトウェア株式会社

兵庫県伊丹市中央3丁目1番17号

(72)発明者 藤岡 宗三

兵庫県伊丹市中央3丁目1番17号 三菱電機セミコンダクタソフトウェア株式会社内

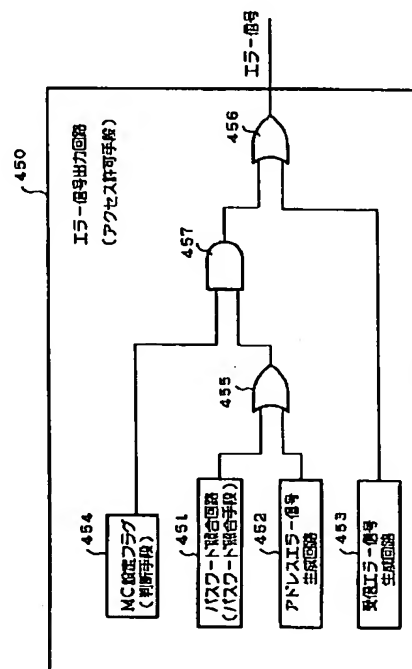
(74)代理人 弁理士 宮田 金雄 (外3名)

(54)【発明の名称】 通信装置

(57)【要約】

【課題】 セキュリティを高くした場合、メモリテストが困難であった。

【解決手段】 製造者コードエリアが設けられたメモリ403と、メモリ403の製造者エリアMAに所定のコードが格納されているときは、パスワードが一致している場合にはリード・ライト装置300からのユーザエリアUAのアクセスを許可し、所定のコードが格納されていない場合には、パスワード照合回路451によるパスワードの照合の結果にかかわらずリード・ライト装置300からのメモリ403のメモリ403全体へのアクセスを許可するように制御するエラー信号出力回路450とを有する非接触式ICカードである。



【特許請求の範囲】

【請求項 1】 外部装置との間で通信を行う通信装置において、第 1 の領域と第 2 の領域とを有するメモリであって、前記第 1 の領域には前記外部装置が前記メモリをアクセスする際に第 1 のパスワードの一致が必要であることを示す所定のコードを格納するための第 3 の領域が設けられているメモリと、前記第 3 の領域に前記所定のコードが格納されているか否かを判断する判断手段と、前記メモリをアクセスする際に前記外部装置から送られてくる第 1 のパスワードと前記通信装置の内部に格納されている第 1 のパスワードとの照合を行うパスワード照合手段と、前記第 3 の領域に前記所定のコードが格納されているときは、前記パスワード照合手段による照合の結果、第 1 のパスワードが一致している場合には前記外部装置からの前記メモリの前記第 2 の領域へのアクセスを許可し、前記第 3 の領域に前記所定のコードが格納されていない場合には、前記パスワード照合手段による第 1 のパスワードの照合の結果にかかわらず前記外部装置からの前記第 1 の領域及び前記第 2 の領域へのアクセスを許可するアクセス許可手段とを具備することを特徴とする通信装置。

【請求項 2】 外部装置との間で通信を行う通信装置において、第 1 の領域と第 2 の領域とを有するメモリであって、前記第 1 の領域には前記外部装置が前記メモリをアクセスする際に第 1 のパスワードの一致が必要であることを示す所定のコードを格納するための第 3 の領域が設けられているメモリと、前記第 3 の領域に前記所定のコードが格納されているか否かを判断する判断手段と、前記メモリの前記第 3 の領域に前記所定のコードが格納されている場合には、前記メモリをアクセスする際に前記外部装置から送られてくる第 1 のパスワードと前記通信装置の内部に格納されている第 1 のパスワードとの照合を行うパスワード照合手段と、前記第 3 の領域に前記所定のコードが格納されているときは、前記パスワード照合手段による照合の結果、第 1 のパスワードが一致している場合に前記外部装置からの前記メモリの前記第 2 の領域へのアクセスを許可し、前記第 3 の領域に前記所定のコードが格納されていない場合には、第 1 のパスワードの照合をせずに前記外部装置からの前記第 1 の領域及び前記第 2 の領域へのアクセスを許可するアクセス許可手段とを具備することを特徴とする通信装置。

【請求項 3】 判断手段は、第 3 の領域に所定のコードが格納されているか否かを、外部装置からの ID コード要求のコマンドを受信してから前記外部装置に ID コードを送出するまでの期間に判断することを特徴とする請求項 1 または請求項 2 記載の通信装置。

【請求項 4】 第 1 の領域には第 2 のパスワードを格納するための第 4 の領域が設けられており、パスワード照合手段は、第 3 の領域に所定のコードが格納されている場合に、外部装置から前記第 4 の領域のアドレスとともに

に第 2 のパスワードが送られてきたときには、前記第 4 の領域に格納されている第 2 のパスワードと前記外部装置から送られてきた第 2 のパスワードとを照合し、アクセス許可手段は、前記パスワード照合手段の照合の結果、第 2 のパスワードが一致した場合には、前記外部装置からの第 1 の領域及び第 2 の領域へのアクセスを第 1 のパスワードの照合の一致を必要とせずに許可することを特徴とする請求項 1 から請求項 3 のうちのいずれか 1 項記載の通信装置。

10 【請求項 5】 第 1 の領域には第 2 のパスワードを格納するための第 4 の領域が設けられており、パスワード照合手段は、第 3 の領域に所定のコードが格納されている場合に、外部装置から前記第 4 の領域のアドレスとともに第 2 のパスワードが送られてきたときには、前記第 4 の領域に格納されている第 2 のパスワードと前記外部装置から送られてきた第 2 のパスワードとを照合し、通信装置はさらに前記パスワード照合手段による第 2 のパスワードの照合の結果、第 2 のパスワードが一致したときから前記外部装置から送られてくるコマンドの数をカウントするカウント手段を具備し、アクセス許可手段は、前記パスワード照合手段の照合の結果、第 2 のパスワードが一致し、且つ、前記カウント手段によってカウントされたコマンドの数が所定の数以上である場合に、前記外部装置からの第 1 の領域及び第 2 の領域へのアクセスを第 1 のパスワードの照合の一致を必要とせずに許可することを特徴とする請求項 1 から請求項 3 のうちのいずれか 1 項記載の通信装置。

30 【請求項 6】 第 1 の領域には第 2 のパスワードを格納するための第 4 の領域が設けられており、パスワード照合手段は、第 3 の領域に所定のコードが格納されている場合に、外部装置から前記第 4 の領域のアドレスとともに第 2 のパスワードが送られてきたときには、前記第 4 の領域に格納されている第 2 のパスワードと前記外部装置から送られてきた第 2 のパスワードとを照合し、通信装置はさらに前記パスワード照合手段による第 2 のパスワードの照合の結果、第 2 のパスワードが一致したときから外部装置から送られてくるコマンドの数をカウントするカウント手段を具備し、アクセス許可手段は、前記パスワード照合手段の照合の結果、第 2 のパスワードが一致し、且つ、前記カウント手段によってカウントされたコマンドの数が第 1 の所定数以上で、且つ、第 2 の所定数以下である場合に、前記外部装置からの第 1 の領域及び第 2 の領域へのアクセスを第 1 のパスワードの照合の一致を必要とせずに許可することを特徴とする請求項 1 から請求項 3 のうちのいずれか 1 項記載の通信装置。

50 【請求項 7】 第 2 のパスワードはメモリからデータを読み出す場合に照合されるリードパスワードと、前記メモリへデータを書き込む場合に照合されるライトパスワードとを含み、第 4 の領域には前記リードパスワードを格納するためのリードパスワード領域と、ライトパスワ

3

ードを格納するためのライトパスワード領域とが設けられ、パスワード照合手段は、第3の領域に所定のコードが格納されているときに、外部装置からリードパスワード領域のアドレスとともにリードパスワードが送られてきた場合には前記リードパスワード領域に格納されているリードパスワードと前記外部装置から送られてきたリードパスワードとを照合し、前記外部装置から前記ライトパスワード領域のアドレスとともにライトパスワードが送られてきた場合には前記ライトパスワード領域に格納されているライトパスワードと前記外部装置から送られてきたライトパスワードとを照合し、アクセス許可手段は、前記パスワード照合手段による照合の結果、リードパスワードが一致した場合には前記外部装置からの第1の領域及び第2の領域のデータの読み出しを第1のパスワードの照合の一致を必要とせずに許可し、前記パスワード照合手段による照合の結果、ライトパスワードが一致した場合には前記外部装置からの前記第1の領域及び前記第2の領域へのデータの書き込みを第1のパスワードの照合の一致を必要とせずに許可することを特徴とする請求項4から請求項6のうちのいずれか1項記載の通信装置。

【請求項8】 第2のパスワードはメモリからデータを読み出す場合に照合されるリードパスワードと、前記メモリへデータを書き込む場合に照合されるライトパスワードとを含み、第4の領域には前記リードパスワードを格納するためのリードパスワード領域と、前記ライトパスワードを格納するためのライトパスワード領域とが設けられ、パスワード照合手段は、第3の領域に所定のコードが格納されているときに、外部装置から前記リードパスワード領域のアドレスとともにリードパスワードが送られてきた場合には前記リードパスワード領域に格納されているリードパスワードと前記外部装置から送られてきたリードパスワードとを照合し、前記外部装置から前記ライトパスワード領域のアドレスとともにライトパスワードが送られてきた場合には前記ライトパスワード領域に格納されているライトパスワードと前記外部装置から送られてきたライトパスワードとを照合し、アクセス許可手段は、前記パスワード照合手段による照合の結果、リードパスワード及びライトパスワードの両方が一致した場合には前記外部装置からの第1の領域及び第2の領域の読み出し及び書き込みの両方を第1のパスワードの照合の一致を必要とせずに許可することを特徴とする請求項4から請求項6のうちのいずれか1項記載の通信装置。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】この発明はプログラマブルメモリを内蔵したLSIを有する非接触式ICカード等の通信装置に関するものである。

【0002】

4

【従来の技術】図25は従来の非接触式ICカードに用いられるプログラマブルメモリ内蔵のLSIのメモリマップを示す図である。同図において、10はメモリ部、11は書き換え可能なプログラマブルメモリ部、12は予めデータが書き込まれており書き換えできない固定メモリ部をそれぞれ示している。同図に示すように、プログラマブルメモリ部11は複数のエリアに分割されている。各エリアにはパスワードが設けられており、各々のエリアをアクセスする場合にはパスワードの照合が行われ、パスワードが一致していない場合にはアクセスが禁止され、パスワードが一致した場合に限りそのパスワードに対応するエリア内のアクセスができるようになって

いる。【0003】このようなLSIでは、ウエハプロセス完了直後はパスワード格納アドレスのデータは不定となり、各エリアをアクセスすることが非常に困難である。このため、ウエハ作成時に固定メモリ部12にマスタパスワードを書き込んでおき、このマスタパスワードを照合して一致すれば、各エリアのパスワードの照合結果にかかわらず全エリアのアクセスを行えるようにするか、パスワードの変更を許可するようになっている。このマスタパスワードを使用してメモリのテストが行われる。

【0004】図26は、従来の非接触式ICカード通信システムの構成を示すブロック図である。同図において、100はリード・ライト装置、200は非接触式ICカードを示している。非接触式ICカード200は、電波を送受信するためのアンテナ201と、搬送波をデータで変調するとともに変調された搬送波からデータを復調する変復調回路202と、データを格納するプログラマブルメモリ203と、非接触式ICカード200の動作を制御してコマンド処理等を実行する制御回路204とを具備している。なお、変復調回路202と、プログラマブルメモリ203と、制御回路204とは非接触式ICカード用のLSI210に組み込まれている。また、プログラマブルメモリ203は図25に示したメモリ部10と同様の構成となっている。

【0005】図27はリード・ライト装置100と非接触式ICカード200との間の通信手順を示すシーケンス図である。同図に示すように、まず、リード・ライト装置100からリードIDコマンド（以下RIDコマンドと記す）が非接触式ICカード200に送られて通信が開始される。次に、リード・ライト装置100からコマンドを非接触式ICカード200に送信する。このコマンドには例えばプログラマブルメモリ203のリードやライトなどのコマンドがある。非接触式ICカード200はこのコマンドを実行し、実行した結果はリード・ライト装置100に送信される。もしコマンドの実行前に通信エラーやパスワードの照合エラーなどのエラーが生じた場合にはコマンドは実行されずにエラーの状態を示すエラーステータスを送信するか、あるいは、リード

・ライト装置100に何も送信しないようにしている。

【0006】

【発明が解決しようとする課題】従来の通信装置は以上のように構成されているので、固定メモリに格納されているパスワードがわかってしまうとメモリ全体のデータのアクセスが可能になり、パスワードの変更もできないなどの課題があった。

【0007】この発明は上記のような課題を解決するためになされたもので、高いセキュリティーを維持しつつ容易にメモリのテストができる通信装置を得ることを目的とする。

【0008】

【課題を解決するための手段】請求項1記載の発明に係る通信装置は、第1の領域と第2の領域とを有するメモリであって、第1の領域には外部装置がメモリをアクセスする際に第1のパスワードの一致が必要であることを示す所定のコードを格納するための第3の領域が設けられているメモリと、第3の領域に所定のコードが格納されているか否かを判断する判断手段と、メモリをアクセスする際に外部装置から送られてくる第1のパスワードと通信装置の内部に格納されている第1のパスワードとの照合を行うパスワード照合手段と、第3の領域に所定のコードが格納されているときは、パスワード照合手段による照合の結果、第1のパスワードが一致している場合には外部装置からのメモリの第2の領域のアクセスを許可し、第3の領域に所定のコードが格納されていない場合には、パスワード照合手段による第1のパスワードの照合の結果にかかわらず外部装置からの第1の領域及び第2の領域へのアクセスを許可するアクセス許可手段とを具備するものである。

【0009】請求項2記載の発明に係る通信装置は、第1の領域と第2の領域とを有するメモリであって、第1の領域には外部装置がメモリをアクセスする際に第1のパスワードの一致が必要であることを示す所定のコードを格納するための第3の領域が設けられているメモリと、第3の領域に所定のコードが格納されているか否かを判断する判断手段と、メモリの第3の領域に所定のコードが格納されている場合には、メモリをアクセスする際に外部装置から送られてくる第1のパスワードと通信装置の内部に格納されている第1のパスワードとの照合を行うパスワード照合手段と、第3の領域に所定のコードが格納されているときは、パスワード照合手段による照合の結果、第1のパスワードが一致している場合に外部装置からのメモリの第2の領域のアクセスを許可し、第3の領域に所定のコードが格納されていない場合には、第1のパスワードの照合をせずに外部装置からの第1の領域及び第2の領域へのアクセスを許可するアクセス許可手段とを具備するものである。

【0010】請求項3記載の発明に係る通信装置は、第3の領域に所定のコードが格納されているか否かを、外

部装置からのIDコード要求のコマンドを受信してから外部装置にIDコードを送出するまでの期間に判断する判断手段を具備するものである。

【0011】請求項4記載の発明に係る通信装置は、第1の領域には第2のパスワードを格納するための第4の領域が設けられたメモリと、第3の領域に所定のコードが格納されている場合に、外部装置から第4の領域のアドレスとともに第2のパスワードが送られてきたときには、第4の領域に格納されている第2のパスワードと外部装置から送られてきた第2のパスワードとを照合するパスワード照合手段と、パスワード照合手段の照合の結果、第2のパスワードが一致した場合には、外部装置からの第1の領域及び第2の領域へのアクセスを第1のパスワードの照合の一致を必要とせずに許可するアクセス許可手段とを具備するものである。

【0012】請求項5記載の発明に係る通信装置は、第1の領域には第2のパスワードを格納するための第4の領域が設けられたメモリと、第3の領域に所定のコードが格納されている場合に、外部装置から第4の領域のアドレスとともに第2のパスワードが送られてきたときには、第4の領域に格納されている第2のパスワードと外部装置から送られてきた第2のパスワードとを照合するパスワード照合手段と、パスワード照合手段による第2のパスワードの照合の結果、第2のパスワードが一致したときから外部装置から送られてくるコマンドの数をカウントするカウント手段と、パスワード照合手段による照合の結果、第2のパスワードが一致し、且つ、カウント手段によってカウントされたコマンドの数が所定の数以上である場合に、外部装置からの第1の領域及び第2の領域へのアクセスを第1のパスワードの照合の一致を必要とせずに許可するアクセス許可手段とを具備するものである。

【0013】請求項6記載の発明に係る通信装置は、第1の領域には第2のパスワードを格納するための第4の領域が設けられたメモリと、第3の領域に所定のコードが格納されている場合に、外部装置から第4の領域のアドレスとともに第2のパスワードが送られてきたときには、第4の領域に格納されている第2のパスワードと外部装置から送られてきた第2のパスワードとを照合するパスワード照合手段と、パスワード照合手段による第2のパスワードの照合の結果、第2のパスワードが一致したときから外部装置から送られてくるコマンドの数をカウントするカウント手段と、パスワード照合手段による照合の結果、第2のパスワードが一致するとともにカウント手段によってカウントされたコマンドの数が第1の所定数以上、且つ、第2の所定数以下である場合に、外部装置からの第1の領域及び第2の領域へのアクセスを第1のパスワードの照合の一致を必要とせずに許可するアクセス許可手段とを具備するものである。

【0014】請求項7記載の発明に係る通信装置は、第

4の領域にはリードパスワードを格納するためのリードパスワード領域と、ライトパスワードを格納するためのライトパスワード領域とが設けられたメモリと、第3の領域に所定のコードが格納されているときに、外部装置からリードパスワード領域のアドレスとともにリードパスワードが送られてきた場合にはリードパスワード領域に格納されているリードパスワードと外部装置から送られてきたリードパスワードとを照合し、外部装置からライトパスワード領域のアドレスとともにライトパスワードが送られてきた場合にはライトパスワード領域に格納されているライトパスワードと外部装置から送られてきたライトパスワードとを照合するパスワード照合手段と、パスワード照合手段による照合の結果、リードパスワードが一致した場合には外部装置からの第1の領域及び第2の領域のデータの読み出しを第1のパスワードの照合の一致を必要とせずに許可し、パスワード照合手段による照合の結果、ライトパスワードが一致した場合には外部装置からの第1の領域及び第2の領域へのデータの書き込みを第1のパスワードの照合の一致を必要とせずに許可するアクセス許可手段とを具備するものである。

【0015】請求項8記載の発明に係る通信装置は、第4の領域にはリードパスワードを格納するためのリードパスワード領域と、ライトパスワードを格納するためのライトパスワード領域とが設けられたメモリと、第3の領域に所定のコードが格納されているときに、外部装置からリードパスワード領域のアドレスとともにリードパスワードが送られてきた場合にはリードパスワード領域に格納されているリードパスワードと外部装置から送られてきたリードパスワードとを照合し、外部装置からライトパスワード領域のアドレスとともにライトパスワードが送られてきた場合にはライトパスワード領域に格納されているライトパスワードと外部装置から送られてきたライトパスワードとを照合するパスワード照合手段と、パスワード照合手段による照合の結果、リードパスワード及びライトパスワードの両方が一致した場合には外部装置からの第1の領域及び第2の領域の読み出し及び書き込みの両方を第1のパスワードの照合の一致を必要とせずに許可するアクセス許可手段とを具備するものである。

【0016】

【発明の実施の形態】以下、この発明の実施の一形態を説明する。

実施の形態1. 図1はこの実施の形態1の非接触式ICカードの通信システムを示す図であり、図において、300はリード・ライト装置（外部装置）、400はリード・ライト装置300との間で電波を用いて通信を行う非接触式ICカード（通信装置）を示している。非接触式ICカード400は、電波を送受信するためのアンテナ401と、搬送波をデータに変調するとともに変調さ

れた搬送波からデータを復調する変復調回路402と、データを格納するプログラマブルメモリ（メモリ）403と、非接触式ICカード400の動作を制御してコマンド処理等を実行する制御回路404とを具備している。なお、変復調回路402と、プログラマブルメモリ403と、制御回路404とは非接触式ICカード用LSI410に組み込まれている。

【0017】図2は非接触式ICカード400のプログラマブルメモリ403のメモリマップを示す図である。図に示すようにアドレスAD0からAD1まではエリアA1、アドレスAD1+1からAD2まではエリアA2、アドレスAD2+1からAD3まではエリアA3となっている。エリアA4、A5についても同様である。また、エリアA1からエリアA5にはそれぞれのエリアをアクセスする場合に照合されるパスワード（第1のパスワード）PW1からPW5がそれぞれ格納されている。なお、エリアA1からエリアA5はユーザエリア（第2の領域）UAを構成する。また、アドレスAD5+1からAD6は製造者エリア（第1の領域）MAであり、特定の値が格納されたときにパスワードを有効にする製造者コード（所定のコード、以下MCと記す）を格納するMCエリア（第3の領域）が確保されている。なお、MCは、例えば、「00H」、「01H」、「03H」、「07H」、「0FH」、「1FH」、「3FH」、「7FH」、「FFH」、「80H」、「C0H」、「E0H」、「F0H」、「F8H」、「FCH」、「FEH」などのウエハプロセス完了後になりやすいコード、あるいは、製品テストでプログラマブルメモリ403に書き込むパターン「00H」、「FFH」、「AAH」、「55H」は避けて、例えば、「12H」、「34H」などのコードを用いる。以下の実施の形態ではMCとして「12H」を用いる場合について説明する。

【0018】次に動作について説明する。まず、製品テスト時のアクセスについて説明する。製品テストはLSIチップ単体で出荷する場合と非接触式ICカード単位で出荷する場合とでMC設定の時期が異なるが、ここでは非接触式ICカード単位で出荷する場合のテストについて説明する。

【0019】図3はリード・ライト装置300と非接触式ICカード400との間の通信手順を示すシーケンス図である。図に示すように、まずリード・ライト装置300から非接触式ICカード400にID読み出しのRIDコマンドを送信する。非接触式ICカード400はRIDコマンドを受信するとプログラマブルメモリ403内の製造者エリアMAのMCエリアに特定の値が格納されているか否かを期間P1の間に確認する。もしMCエリアに特定のコード「12H」が格納されていれば、それ以降のコミュニケーションにおいてはリード・ライト装置300からのアクセスはパスワードの照合が必要になる。MCエリアに特定のコード「12H」が格納されて

いない場合には、それ以降のリード・ライト装置300からのアクセスはパスワードの照合の結果が一致していなくても許可される。

【0020】さて、MCエリアに特定のコード「12H」が格納されているか否かの確認処理が終了した後、非接触式ICカード400は自身のIDコードをリード・ライト装置300に送出する。次に、リード・ライト装置300は非接触式ICカード400から送られたIDコードを確認してコミュニケーションをとるべき相手であると判断されると所定の処理を要求するコマンドを非接触式ICカード400に送出する。

【0021】図4はこのコマンドを非接触式ICカード400が受信したときのエラー処理を実行する制御回路404内のエラー信号出力回路（アクセス許可手段）450の構成を示す図である。図において、451は格納されているパスワードと入力されたパスワードの照合を行い、パスワードが一致しない場合に「H」レベルのパスワードエラー信号を出力するパスワード照合回路（パスワード照合手段）、452は非接触式ICカード400から許可された範囲外のアドレスが指定されたときに「H」レベルのアドレスエラー信号を出力するアドレスエラー信号生成回路、453は信号の受信にエラーが生じた場合に「H」レベルの受信エラー信号を出力する受信エラー信号生成回路、454はMCエリアに特定のコード「12H」が格納された場合には「H」信号が格納され、その他のコードが格納されている場合には「L」レベル信号が格納されるMC設定フラグ（判断手段）、455及び456はオアゲート、457はアンドゲートである。なお、実際にはMC設定フラグ454の値のセットの判断は制御回路404によって行われて値がMC設定フラグ454に書き込まれる。MCエリアに特定コード「12H」が書き込まれる前はMCエリアには、例えば、「FFH」等が書き込まれている。このときMC設定フラグ454は「L」信号を出力する。このため、アンドゲート457ではパスワード照合回路451から出力されるパスワードエラー信号及びアドレスエラー信号生成回路452から出力されるアドレスエラー信号はマスクされオアゲート456からは受信エラーがあった場合にのみ「H」レベルのエラー信号を出力される。このため、パスワードエラー、アドレスエラーが生じた場合であって受信エラーが生じていなければエラー処理は行われない。従って非接触式ICカード400のメモリのテスト時にはパスワードが一致しなくてもアドレスAD0からアドレスAD6までの領域をアクセスすることができる。すなわちエラー信号出力回路450は外部からのアクセスに対して、そのアクセスを許可するか禁止するかを決定する動作を行う。

【0022】次に、テストが終了し、MCエリアに特定のコード「12H」が書き込まれた後はMC設定フラグ454に「H」レベル信号が書き込まれ、パスワードエラ

ー信号、アドレスエラー信号、受信エラー信号のうち、いずれか1つの信号が「H」レベルとなったときにオアゲート456から「H」レベルのエラー信号が出力される。従って、MCエリアに特定のコード「12H」が書き込まれた後はパスワードが一致し、且つ、プログラブルメモリ403のアドレスAD0からアドレスAD5の範囲のアドレスを指定したときのみアクセスが許可される。

【0023】図5はリード・ライト装置300から非接触式ICカード400にリードコマンドを転送した場合の通信手順を示すシーケンス図である。また、図6はリードコマンド510の構成を示す図である。図6に示すようにリードコマンド510はコマンドコード511、読み出すデータのアドレス512、及びパスワード513から構成される。さらに、図7はリードコマンド510がリード・ライト装置300から送信されてきた場合に非接触式ICカード400からリード・ライト装置300に送信されるリードデータ520の構成を示す図である。図7に示すようにリードデータ520はエラーの状態を示すエラーステータス521及び読み出したリードデータ列522から構成されている。

【0024】図5に示すように、リード・ライト装置300から非接触式ICカード400にRIDコマンドが送られることによってリード・ライト装置300と非接触式ICカード400との間のデータ通信が開始される。非接触式ICカード400はRIDコマンドを受信すると図3を用いて説明したようにMCエリアに特定のコード「12H」が格納されているか否かの判定と、この判定の結果に応じた処理とが期間P2で行われる。その後、自身のIDコードをリード・ライト装置300に対して送信する。次に、リード・ライト装置300から非接触式ICカード400にリードコマンド510を送出すると非接触式ICカード400はMCエリアに「12H」が格納されている場合にはパスワード513が照合一致した場合に限りリードコマンド510のアドレス512に対応するプログラブルメモリ403のデータをエラーステータス521とともにリードデータ520としてリード・ライト装置300に送出する。MCエリアに「12H」が格納されていなければパスワード513の照合の結果にかかわらずアクセスが許可され、リードデータ520として送出される。

【0025】リード・ライト装置300から非接触式ICカード400にライトコマンドを送信する場合もリードコマンドの場合と同様である。図8はライトコマンド530の構成を示す図である。図に示すようにライトコマンド530は、コマンドコード531、書き込むべきアドレス532、パスワード533、ライトデータ列534とから構成される。さらに、非接触式ICカード400からライトコマンド530が実行された場合にエラーステータスを返送する。この場合もMCエリアに「12

H」が格納されている場合にはコマンドの実行にはパスワード533の照合一致が必要になり、MCエリアに「12H」が格納されていなければパスワード533が一致しなくてもライトコマンド530が実行される。

【0026】以上説明したように、この実施の形態1ではパスワード付きで送られてきたコマンドについてはMCエリアに特定のコード「12H」が設定されていない場合にはパスワードの照合の結果、一致していなくてもエラーとはならない。従って、同じパスワードで、(どんなパスワードを送っても) プログラブルメモリ403の全エリアのリード及びライトができるので出荷前のメモリの製品テストを容易に行うことができるという効果がある。さらに一旦MCエリアに特定のコード「12H」が設定された場合にはパスワードが一致しなければプログラブルメモリ403のリード及びライト等のアクセスが禁止されるので高いセキュリティを維持することが可能になるという効果がある。

【0027】実施の形態2. この実施の形態2の基本的構成は実施の形態1と同様である。ただし、以下の点で実施の形態1とは異なっている。すなわち、実施の形態1ではMCエリアに特定コードが設定されていない場合であってもリードコマンド510、ライトコマンド530を受信したときにパスワードの照合を行っていたが、この実施の形態2ではリードコマンド、ライトコマンドなどを受信したときにパスワードの照合を省略するように制御回路404を構成したものである。

【0028】図9はこの実施の形態2のMCエリアの設定状態によってパスワード照合の実行の有無を決定する場合の動作を示すフローチャートである。図に示すようにMCエリアに特定のコード「12H」が格納されていない場合(ステップST901)にはパスワードの照合をせずにコマンド処理を実行する(ステップST902)。一方、MCエリアに特定のコード「12H」が格納されている場合にはパスワードの照合を行い(ステップST903)、パスワードが一致している場合には(ステップST904)、コマンド処理を実行し、パスワードが一致していなかった場合には(ステップST904)、パスワードエラー処理を実行する(ステップST905)。

【0029】図10はMCエリアに特定のコード「12H」が設定されていない場合にリード・ライト装置300から非接触式ICカード400に送信するリードコマンド540の構成を示す図である。図に示すようにリードコマンド540はコマンドコード541と、読み出すべきアドレス542が送信されるのみであり、パスワードは送信されない。

【0030】以上のように、この実施の形態2ではMCエリアに特定のコード「12H」が設定されていない場合にはパスワードを送信する必要がなく、また、パスワードの照合の時間も必要なくなるのでテスト時間を短縮す

ることが可能になるという効果がある。

【0031】実施の形態3. この実施の形態3の基本的構成は実施の形態1と同様である。ただし、プログラブルメモリ403と制御回路404とが以下の点で実施の形態1とは異なっている。

【0032】図11はこの実施の形態3のプログラブルメモリ403の構成を示すメモリマップを示す図である。図に示すようにこの実施の形態3では製造者エリアMAはMC用のMCエリアと製造者リードパスワード

(第2のパスワード、以下MRPと記す)用のMRPエリア(第4の領域)、製造者ライトパスワード(第2のパスワード、以下MWPと記す)用のMWPエリア(第4の領域)とから構成されている。MRP、MWPについては以下に詳細に説明する。

【0033】図12は制御回路404内に設けられたリードコマンドが入力された場合のエラー処理を実行するためのリードコマンド受信時のエラー信号出力回路(アクセス許可手段)460の構成を示す図である。図において、461はプログラブルメモリ403の製造者エリアMAに格納されているMRPが入力されたMRPと一致した場合に「H」信号が格納され、一致しない場合には「L」レベル信号が格納されるMRP照合一致フラグ、462及び、463はオアゲート、464はナンドゲート、465はアンドゲートを示している。なお、ナンドゲート464にはMRP照合一致フラグ461からの出力信号とリードコマンドを受信したときに「H」になるリードコマンド信号が入力される。従って、リードコマンドを受信時にMRPが一致した場合にはパスワードエラー及びアドレスエラーがあってもアンドゲート465でマスクされてその他のエラーがない場合にはエラー信号はオアゲート463からは出力されず、エラー処理は行われない。

【0034】図13は制御回路404内に設けられた、ライトコマンドが入力された場合のエラー処理を実行するためのライトコマンド受信時のエラー信号出力回路(アクセス許可手段)470の構成を示す図である。図において471はプログラブルメモリ403の製造者エリアMAに格納されているMWPが入力されたMWPと一致した場合に「H」信号が格納され、一致しない場合には「L」レベル信号が格納されるMWP照合一致フラグを示している。なお、ナンドゲート474にはMWP照合一致フラグ471からの出力信号とライトコマンドを受信したときに「H」になるライトコマンド信号が入力される。従って、ライトコマンドを受信時にMRPが一致した場合にはパスワードエラー及びアドレスエラーがあってもアンドゲート475でマスクされて、その他のエラーがない場合にはエラー信号はオアゲート473からは出力されず、エラー処理は行われない。なお、MRP照合一致フラグ461及びMWP照合一致フラグ471はリセット信号によって「L」レベルにリセット

13

されるように構成されている。

【0035】図14はリード・ライト装置300と非接触式ICカード400との間のリード動作時の通信手順を示すシーケンス図である。リード・ライト装置300から非接触式ICカード400にRIDコマンドを送出して非接触式ICカード400がIDコードをリード・ライト装置300に返送してくるまでの動作は実施の形態1で説明したとおりである。なお、非接触式ICカード400はコミュニケーション開始前にリセットから解除され、コミュニケーション終了時に再びリセットされる。従って、MRP照合一致フラグ461及びMWP照合一致フラグ471は通信開始前には「L」レベルにリセットされた状態になる。

【0036】次に、リード・ライト装置300は非接触式ICカード400にMRP照合のためのリードコマンドを送出する。図15はリードコマンドの構成を示す図である。図に示すようにリードコマンド550はコマンドコード551、製造者エリアMAのMRPのアドレス552、MRP553から構成される。非接触式ICカード400がこのリードコマンド550を受信すると、MRPを照合して一致した場合には期間P3でMRP照合一致フラグ461を「H」にセットし、一致しなかった場合には「L」のままとする。さらに、このリードコマンド550では製造者エリアMAのアドレス552を指定しているのでアドレス552がアクセス禁止領域となり、アドレスエラーを示すエラーステータスをリード・ライト装置300に返送する。すなわち、この時点では非接触式ICカード400の外部からはアドレスエラーが発生したリードコマンドと認識される。なお、以上の説明では、リード・ライト装置300からリードコマンド550で直接製造者エリアMAのアドレス552を指定するようにしたが、予め定められたユーザエリアUA以外の任意のアドレスをリード・ライト装置300から非接触式ICカード400に送信するようにしても良い。この場合には非接触式ICカード400は予め定められたアドレスをリードコマンドとして受信した場合に製造者エリアMAのMRPのアドレスのリードアクセスとして認識するように構成する。このように構成することで、必ずしもユーザエリアUAの近くの領域である製造者エリアMAの実アドレスを送信しなくても良いのでさらに高いセキュリティを得ることができる。

【0037】次に、リード・ライト装置300からリードコマンド550を非接触式ICカード400に送信するとMRP照合一致フラグ461が「H」にセットされている場合には、パスワードが不一致であってもエラー処理は行われずにプログラマブルメモリ403のすべてのアドレスのリードが許可され、対応するアドレスのデータがリード・ライト装置300に送信される。なお、MRP照合一致フラグ461が「L」のままの場合には、パスワードが一致した場合のみプログラマブルメモ

14

リ403のアドレスAD0からアドレスAD5の領域のリードが許可される。

【0038】図16はリード・ライト装置300と非接触式ICカード400との間のライト動作時の通信手順を示すシーケンス図である。リード・ライト装置300から非接触式ICカード400にRIDコマンドを送出して非接触式ICカード400がIDコードをリード・ライト装置300に返送してくるまでの動作は実施の形態1で説明したとおりである。

10 【0039】次に、リード・ライト装置300は非接触式ICカード400にMWP照合のためのリードコマンドを送出する。図17はこのリードコマンドの構成を示す図である。図に示すようにリードコマンド560はコマンドコード561、製造者エリアMAのMWPのアドレス562、MWP563から構成される。非接触式ICカード400がこのリードコマンド560を受信すると、MWPを照合して一致した場合には期間P4でMWP照合一致フラグ471を「H」にセットし、一致しなかった場合には「L」のままとする。さらに、このリードコマンド560では製造者エリアMAのアドレス562を指定しているのでアクセスアドレスは禁止領域となり、アドレスエラーを示すエラーステータスをリード・ライト装置300に返送する。すなわち、この時点では非接触式ICカード400の外部からはアドレスエラーが発生したリードコマンドと認識される。

20 【0040】次にリード・ライト装置300からライトコマンド560を非接触式ICカード400に送信するとMWP照合一致フラグ471が「H」にセットされている場合には、パスワードが不一致であってもエラー処理は行われずにプログラマブルメモリ403のすべてのアドレスの書き込みが許可され、対応するアドレスにデータが書き込まれる。その後、リード・ライト装置300にエラーステータスデータを送出し、エラーの状態および書き込みが終了したことを通知する。なお、MWP照合一致フラグ471が「L」のままである場合には、各エリアのパスワードが一致した場合のみアドレスAD0からアドレスAD5の領域の書き込みが許可される。

30 【0041】以上のように、この実施の形態3では、例えば、不良解析などのためMCエリアに特定コード「12H」が設定された後でも一定の手続きを経てパスワードエラー、アドレスエラーを無視することができるので高いセキュリティを保ちつつ不良解析時のテストを容易にすることができる効果がある。

【0042】実施の形態4. この実施の形態4は上述した実施の形態3と基本的構成は同じである。ただし以下の点で実施の形態3とは異なっている。

40 【0043】図18はこの実施の形態4の非接触式ICカード400の制御回路404内のリードコマンド受信時のエラー信号出力回路（アクセス許可手段）460aの構成を示す図である。図において、466はMRP照

合後に受信したリードコマンドの回数をカウントするコマンドカウンタ（カウント手段）、467はカウントされたコマンドの回数が所定値以上であるか否かを判定する比較回路、465aは3入力ナンドゲートを示している。なお、図12と同一の部分には同一の符号を付し、重複する説明は省略する。

【0044】図19はリード・ライト装置300と非接触式ICカード400との間の通信手順を示すシーケンス図である。図に示すようにRIDコマンドをリード・ライト装置300が非接触式ICカード400に送って通信が開始されてから期間P3後に非接触式ICカード400がエラーステータスを返送するまでは実施の形態3と同様である。その後リード・ライト装置300から非接触式ICカード400にリードコマンドが送られるとコマンドカウンタ466がカウントし、カウント値を出力する。コマンドカウンタ466がnを越えるカウント値を出力すると比較回路467は「H」レベルの信号を出力する。すなわち、MRP照合一致フラグ461がセットされてからn個（nは整数）のリードコマンドまではパスワードエラー、アドレスエラーは有効であるがn+1回目以降のリードコマンドはパスワードエラー、アドレスエラーがあってもエラー信号は発生されずに実行される。従って、この実施の形態4ではn回のリードコマンドがあった後に始めてリードコマンドがパスワードの照合一致を必要とせずに実行されることを知らない第三者に対するセキュリティを向上させることができる。

【0045】同様にしてライトコマンドに対してもn回のMWPの照合フラグがセットされた後、n個（nは整数）のライトコマンドまではパスワードエラー、アドレスエラーは有効であるが、n+1回目以降のライトコマンドはパスワードエラー、アドレスエラーがあってもエラー信号は発生されずに実行されるように構成される。図20はこの場合のエラー信号出力回路（アクセス許可手段）470aの構成を示す図であり、476はMWP照合一致フラグ471がセットされた後にライトコマンドの数をカウントするコマンドカウンタ（カウント手段）、477はコマンドカウンタ476から出力されるライトコマンドの数がn個に達したら「H」レベルの信号を出力する比較回路である。従って、この実施の形態4ではn回のライトコマンドがあった後に始めてライトコマンドがパスワードの照合一致を必要とせずに実行されることを知らない第三者に対するセキュリティを向上させることができる。

【0046】以上説明したように、この実施の形態4ではさらに高いセキュリティを維持しつつメモリテストを容易にできる効果がある。

【0047】実施の形態5. この実施の形態5は上述した実施の形態4と基本的構成は同じである。ただし以下の点で実施の形態4とは異なっている。すなわち、実施

の形態4では比較回路467及び比較回路477は所定のカウンタ値nを越えた場合に、「H」レベルの信号を出力するように構成した。しかしフラグがセットされてからコマンドの回数がi以上j以下の場合に（i、jは整数）、「H」レベルの信号を維持し、j+1回目以降は「L」レベルの信号を出力するようにしても良い。この場合にはフラグがセットされてからi回目からj回目までのリードコマンドまたはライトコマンドのアクセスはパスワードが一致しなくても許可される。そしてj+1回目以降のコマンドはパスワードの照合の結果一致することが必要になる。

【0048】以上説明したように、この実施の形態5によれば、さらにセキュリティを高くしつつ容易にメモリのテストをすることができる効果がある。

【0049】実施の形態6. この実施の形態6は上述した実施の形態3と基本的構成は同様である。ただし以下の点で実施の形態3とは異なっている。すなわち、実施の形態3では、MRP、MWPを独立して設定したが、この実施の形態6ではMRP、MWPの両方を照合して、両方とも一致すれば、それ以降はリードコマンド、ライトコマンドの両方をプログラブルメモリ403のすべてのエリアに対してパスワードが一致しなくてもエラーとなることなしに実行することができる。

【0050】図21は制御回路404のエラー信号発生回路（アクセス許可手段）480の構成を示す回路図である。図において、481はMRP照合一致フラグ461の出力とMWP照合一致フラグ471の出力とが入力されるアンドゲートである。なお、図12、図13と同一の部分には同一の符号を付し、重複する説明は省略する。

【0051】図22はこの実施の形態6のリード・ライト装置300と非接触式ICカード400との間の通信手順を示すシーケンス図である。図に示すようにIDコードの確認後にMRP照合のためのリードコマンドをリード・ライト装置300から非接触式ICカード400に送ってMRPの照合を行い、次にMWP照合のためのリードコマンドを送ってMWPの照合を行う。MRPとMWPの両方が、照合の結果、一致した場合にリード・ライト装置300からのリードコマンド及びライトコマンドがパスワードPW1からPW5の照合の結果にかかわらずプログラブルメモリ403のすべてのアドレスに対して実行できる。また、実施の形態2で説明したようにパスワードの照合を省略するようにすることもできる。

【0052】実施の形態7. この実施の形態7は上述した実施の形態6と基本的構成は同じである。ただし以下の点で実施の形態6とは異なっている。すなわち、上述した実施の形態6ではMRPとMWPの照合の結果、両方とも一致した場合、その後は、リードコマンド及びライトコマンドがパスワードPW1からPW5の照合の結果

果、一致していなくても実行するように構成したが、この実施の形態 7 では MRP と MWP の照合の結果、両方とも一致した場合、その後、所定の n 個 (n は整数) のコマンドはパスワードの照合が必要であるが、 $n+1$ 回目以降のリードコマンド及びライトコマンドはパスワードの照合の一致を必要とせずに実行することができるように構成している。

【0053】図 23 はこの実施の形態 7 の非接触式 IC カード 400 の制御回路 404 内に設けられたエラー信号出力回路 (アクセス許可手段) 480a の構成を示すブロック図である。図 21 に示すエラー信号出力回路 480 と同一の部分には同一の符号を付し、重複する説明は省略する。図において、484 は MRP 照合一致フラグ 461 と MWP 照合一致フラグ 471 の両方が「H」にセットされた後、非接触式 IC カード 400 が受信したリードコマンドまたはライトコマンドの数をカウントするコマンドカウンタ (カウント手段)、482 はコマンドカウンタ 484 から出力されるカウント値が n (n は整数) を越えると「H」レベルの信号を出力する比較回路、483 は MRP 照合一致フラグ 461、MWP 照合一致フラグ 471、及び比較回路 482 の出力が入力される 3 入力ナンドゲートである。

【0054】次に動作について説明する。図 24 はこの実施の形態 7 の非接触式 IC カード 400 とリード・ライト装置 300 との間の通信手順を示すシーケンス図である。同図に示すように MRP の照合及び MWP の照合については実施の形態 6 と同様である。

【0055】MRP の照合及び MWP の照合の結果、両者とも一致している場合には MRP 照合一致フラグ 461、MWP 照合一致フラグ 471 がともに「H」にセットされる。そしてその後リードコマンドまたはライトコマンドがリード・ライト装置 300 から送られてくるとコマンドカウンタ 484 は入力されたコマンドの数をカウントして、カウント値を出力する。比較回路 482 は入力されたコマンドの数が n を越えると「H」レベル信号を出力する。このため、 $n+1$ 回目からのコマンドについてはパスワードの照合結果に関係なくリード・ライト装置 300 からのリードコマンド及びライトコマンドがプログラブルメモリ 403 のすべてのアドレスに対して実行できる。また、実施の形態 5 で説明したように MRP 照合一致フラグ 461、MWP 照合一致フラグ 471 がセットされた後、 i 回目から j 回目 (i, j は整数) までのコマンドのみ許可するようにしても良い。さらに、実施の形態 2 で説明したようにパスワードの照合を省略するようにすることもできる。

【0056】以上説明したように、この実施の形態 7 では、MRP と MWP が両方とも一致してはじめてメモリのアクセスが許可されるのでさらにセキュリティを高くできるという効果がある。

【0057】

【発明の効果】以上のように、請求項 1 記載の発明によれば、アクセス許可手段を、メモリの所定の領域に所定のコードが格納されているときは、第 1 のパスワードが一致している場合には外部装置からのメモリの第 2 の領域のアクセスを許可し、所定のコードが格納されていない場合には、パスワード照合手段による第 1 のパスワードの照合の結果にかかわらず外部装置からのメモリの第 1 及び第 2 の領域へのアクセスを許可するように構成したので、高いセキュリティを維持しつつメモリのテストを容易にすることができる効果がある。

【0058】請求項 2 記載の発明によれば、アクセス許可手段を、メモリの所定の領域に所定のコードが格納されているときは、パスワード照合手段による照合の結果、第 1 のパスワードが一致している場合に外部装置からのメモリの第 2 の領域のアクセスを許可し、所定のコードが格納されていない場合には、第 1 のパスワードの照合をせずに外部装置からのメモリの第 1 及び第 2 の領域へのアクセスを許可するように構成したので、高いセキュリティを維持しつつメモリのテストを容易、高速にすることができる効果がある。

【0059】請求項 3 記載の発明によれば、判断手段を、メモリの所定の領域に所定のコードが格納されているか否かを、外部装置からの ID コード要求のコマンドを受信してから外部装置に ID コードを送出するまでの期間に判断するように構成したので所定のコードが格納されているか否かの判断を確実にして高いセキュリティを維持できる効果がある。

【0060】請求項 4 記載の発明によれば、アクセス許可手段を、メモリの所定領域に所定のコードが格納されている場合であっても、第 2 のパスワードが一致した場合には外部装置からのメモリの第 1 の領域及び第 2 の領域へのアクセスを第 1 のパスワードの照合の一致を必要とせずに許可するように構成したので、高いセキュリティを維持しつつメモリのテストをさらに容易にすることができる効果がある。

【0061】請求項 5 記載の発明によれば、アクセス許可手段を、メモリの所定領域に所定のコードが格納されている場合であっても、第 2 のパスワードが一致し、且つ、カウント手段によってカウントされたコマンドの数が所定の数以上である場合には外部装置からのメモリの第 1 の領域及び第 2 の領域へのアクセスを第 1 のパスワードの照合の一致を必要とせずに許可するように構成したので、高いセキュリティを維持しつつメモリのテストをさらに容易にすることができる効果がある。

【0062】請求項 6 記載の発明によれば、アクセス許可手段を、メモリの所定領域に所定のコードが格納されている場合であっても、第 2 のパスワードが一致し、且つ、外部装置から送られてきたコマンドの数が第 1 の所定数以上で、且つ、第 2 の所定数以下である場合に、外部装置からのメモリの第 1 の領域及び第 2 の領域へのア

アクセスを第1のパスワードの照合の一致を必要とせずに許可するように構成したので、高いセキュリティを維持しつつメモリのテストをさらに容易にすることができる効果がある。

【0063】請求項7記載の発明によれば、アクセス許可手段を、メモリの所定領域に所定のコードが格納されている場合であっても、リードパスワードが一致した場合には外部装置からのメモリの第1の領域及び第2の領域のデータの読み出しを第1のパスワードの照合の一致を必要とせずに許可し、ライトパスワードが一致した場合には外部装置からのメモリの第1の領域及び第2の領域へのデータの書き込みを第1のパスワードの照合の一致を必要とせずに許可するように構成したので、高いセキュリティを維持しつつメモリのテストをさらに容易にすることができる効果がある。

【0064】請求項8記載の発明によれば、アクセス許可手段を、メモリの所定領域に所定のコードが格納されている場合であっても、リードパスワード及びライトパスワードの両方が一致した場合には外部装置からのメモリの第1の領域及び第2の領域の読み出し及び書き込みの両方を第1のパスワードの照合の一致を必要とせずに許可するように構成したので、高いセキュリティを維持しつつメモリのテストをさらに容易にすることができる効果がある。

【図面の簡単な説明】

【図1】 この発明の実施の形態1の非接触式ICカードの通信システムを示す図である。

【図2】 実施の形態1の非接触式ICカードのプログラマブルメモリのメモリマップを示す図である。

【図3】 実施の形態1のリード・ライト装置と非接触式ICカードとの間の通信手順を示すシーケンス図である。

【図4】 実施の形態1においてコマンドを非接触式ICカードが受信したときのエラー処理を実行する制御回路内のエラー信号生成回路の構成を示す図である。

【図5】 実施の形態1のリード・ライト装置から非接触式ICカードにリードコマンドを転送した場合の通信手順を示すシーケンス図である。

【図6】 リードコマンドの構成を示す図である。

【図7】 リードコマンドがリード・ライト装置から送信されてきた場合に非接触式ICカードからリード・ライト装置に送信されるリードデータの構成を示す図である。

【図8】 ライトコマンドの構成を示す図である。

【図9】 この発明の実施の形態2のMCエリアの設定状態によってパスワード照合の実行の有無を決定する場合動作を示すフローチャートである。

【図10】 実施の形態2においてMCエリアに特定のコードが設定されていない場合にリード・ライト装置から非接触式ICカードに送信するリードコマンドの構成

を示す図である。

【図11】 この発明の実施の形態3のプログラマブルメモリの構成を示すメモリマップを示す図である。

【図12】 実施の形態3の制御回路内に設けられたリードコマンドが入力された場合のエラー処理を実行するためのリードコマンド受信時のエラー信号出力回路の構成を示す図である。

【図13】 実施の形態3の制御回路内に設けられたライトコマンドが入力された場合のエラー処理を実行するためのライトコマンド受信時のエラー信号出力回路の構成を示す図である。

【図14】 実施の形態3におけるリード・ライト装置と非接触式ICカードとの間のリード動作時の通信手順を示すシーケンス図である。

【図15】 MRP照合のためのリードコマンドの構成を示す図である。

【図16】 実施の形態3におけるリード・ライト装置と非接触式ICカードとの間のライト動作時の通信手順を示すシーケンス図である。

【図17】 MWP照合のためのリードコマンドの構成を示す図である。

【図18】 この発明の実施の形態4の非接触式ICカードの制御回路内のリードコマンド受信時のエラー信号出力回路の構成を示す図である。

【図19】 実施の形態4におけるリード・ライト装置と非接触式ICカードとの間の通信手順を示すシーケンス図である。

【図20】 実施の形態4のエラー信号出力回路の構成を示す図である。

【図21】 この発明の実施の形態6のエラー信号発生回路の構成を示す図である。

【図22】 実施の形態6におけるリード・ライト装置と非接触式ICカードとの間の通信手順を示すシーケンス図である。

【図23】 この発明の実施の形態7の非接触式ICカードの制御回路内に設けられたエラー信号出力回路の構成を示す図である。

【図24】 実施の形態7における非接触式ICカードとリード・ライト装置との間の通信手順を示すシーケンス図である。

【図25】 従来の非接触式ICカードに用いられるプログラマブルメモリ内蔵のLSIのメモリマップを示す図である。

【図26】 従来の非接触式ICカード通信システムの構成を示す図である。

【図27】 従来のリード・ライト装置と非接触式ICカードとの間の通信手順を示すシーケンス図である。

【符号の説明】

300 リード・ライト装置（外部装置）、400 非接触式ICカード（通信装置）、403 プログラマブル

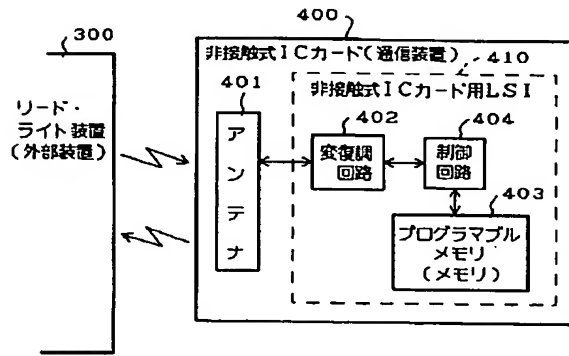
21

ルメモリ（メモリ）、450、460、460a、470、470a、480、480a エラー信号出力回路（アクセス許可手段）、451 パスワード照合回路（パスワード照合手段）、454 MC設定フラグ（判

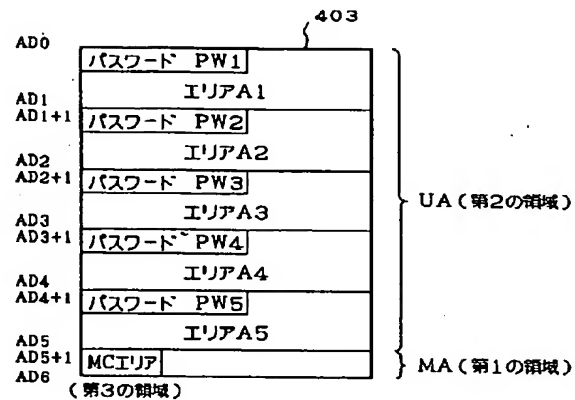
22

断手段）、466、476、484 コマンドカウンタ（カウント手段）、MA 製造者エリア（第1の領域）、UA ユーザエリア（第2の領域）。

【図1】



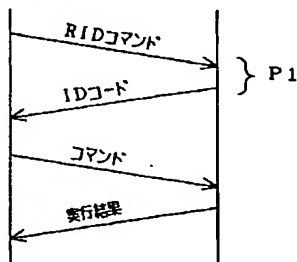
【図2】



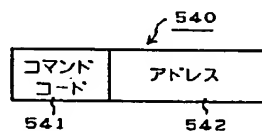
【図3】

MA: 製造者エリア (第1の領域)
UA: ユーザエリア (第2の領域)

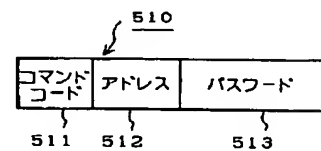
リード・ライト装置 非接触式ICカード



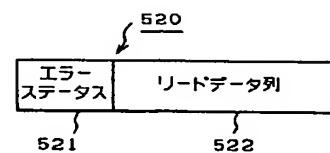
【図10】



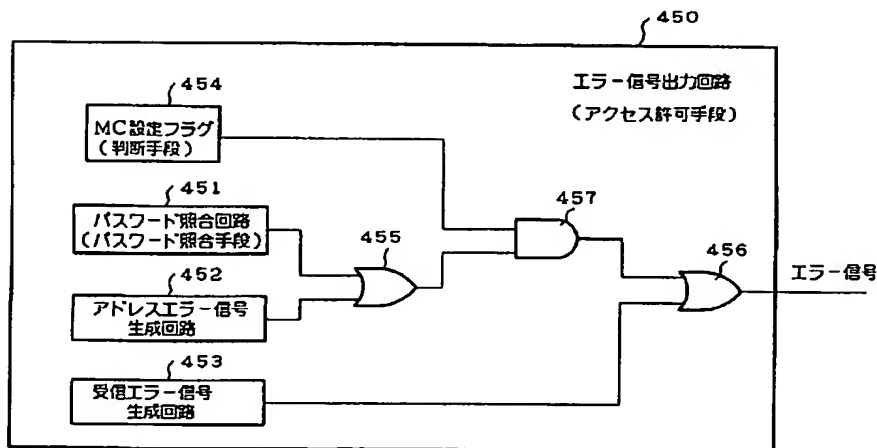
【図6】



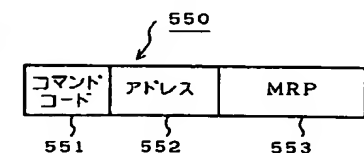
【図7】



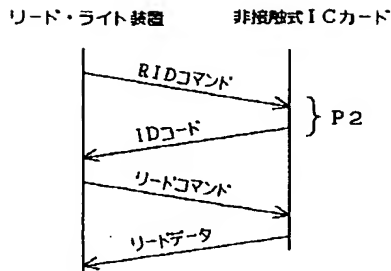
【図4】



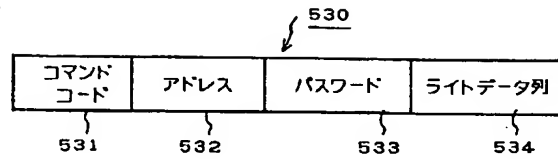
【図15】



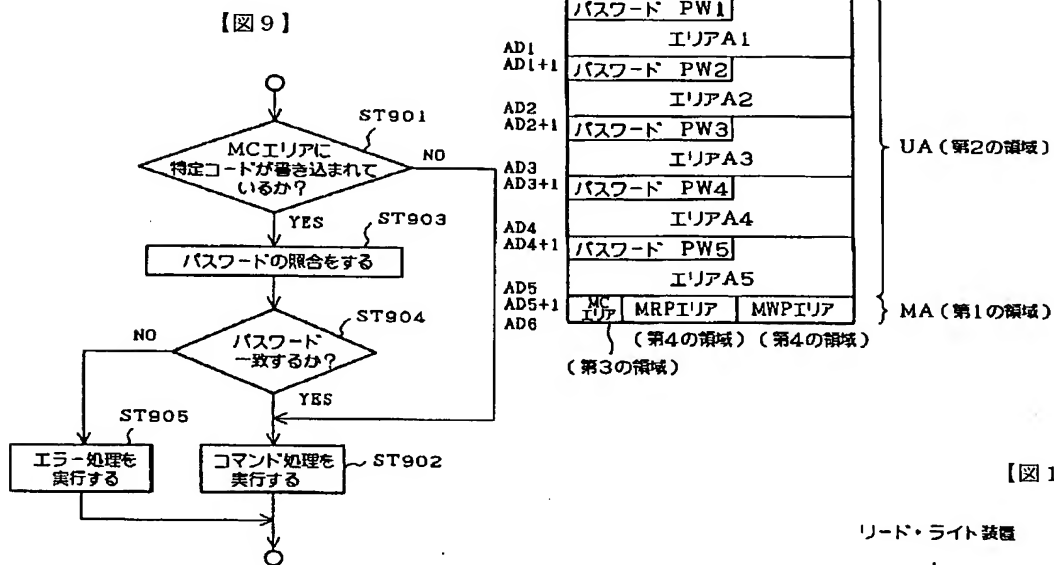
【図5】



【図8】

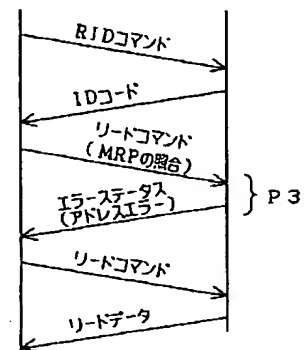


【図11】

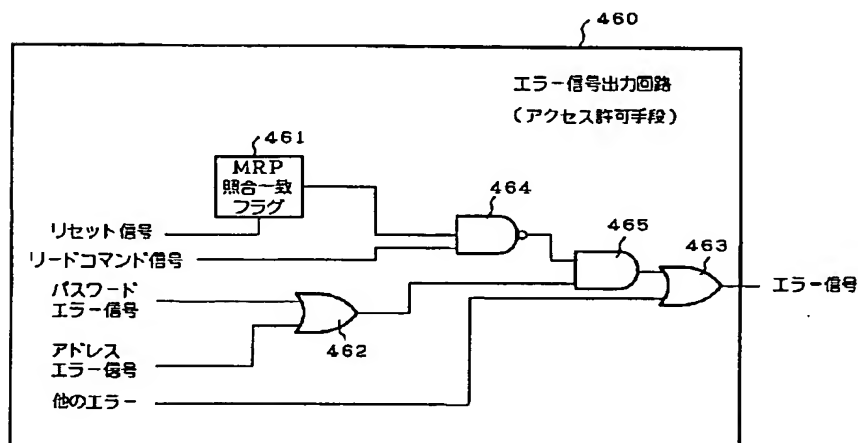


【図14】

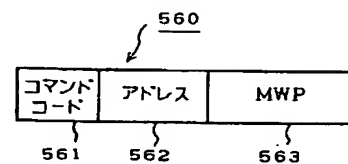
リード・ライト装置 非接触式ICカード



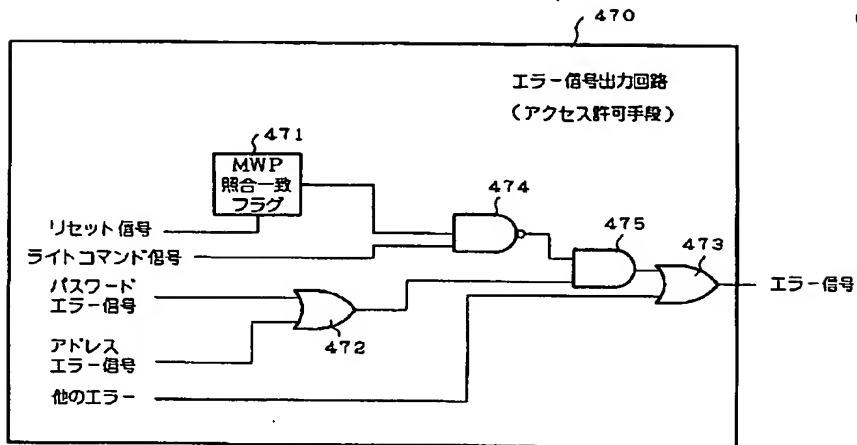
【図12】



【図17】

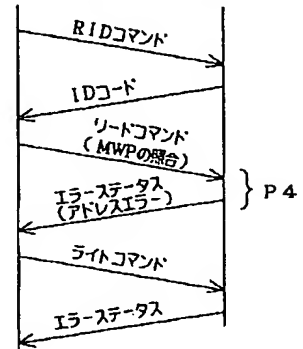


【図13】



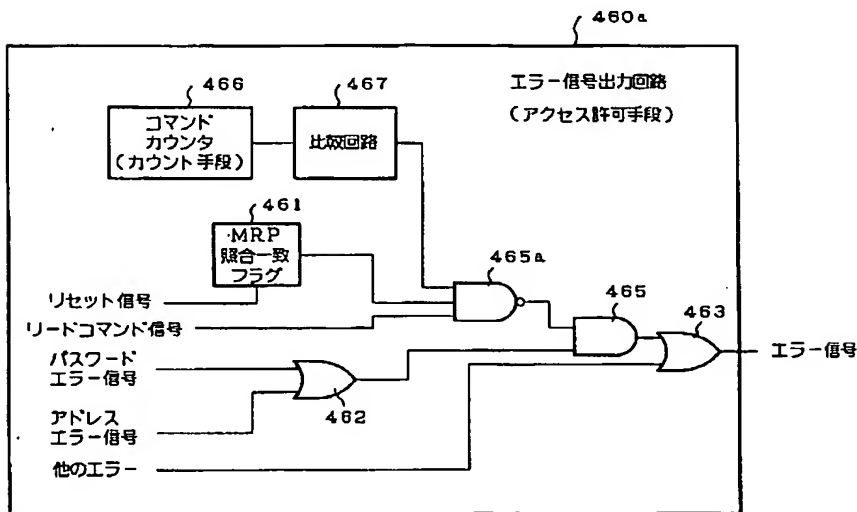
【図16】

リード・ライト装置 非接触式ICカード

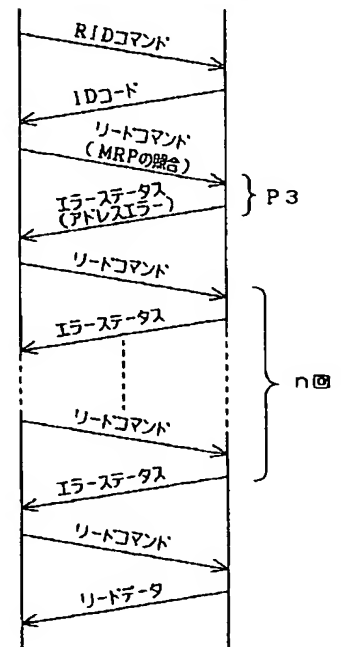
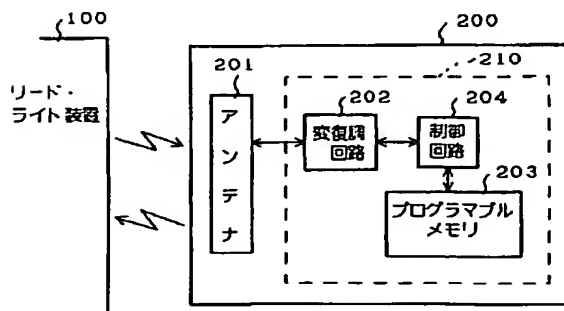


【図19】

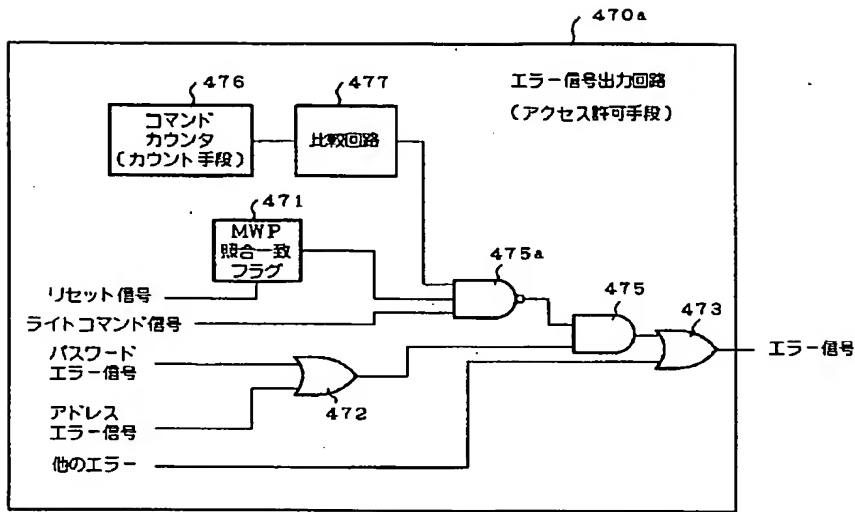
リード・ライト装置 非接触式ICカード



【図26】

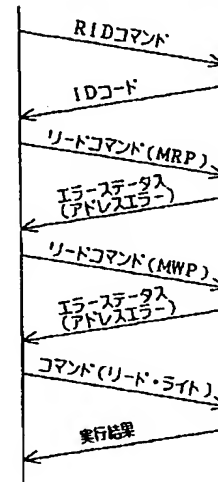


【図20】

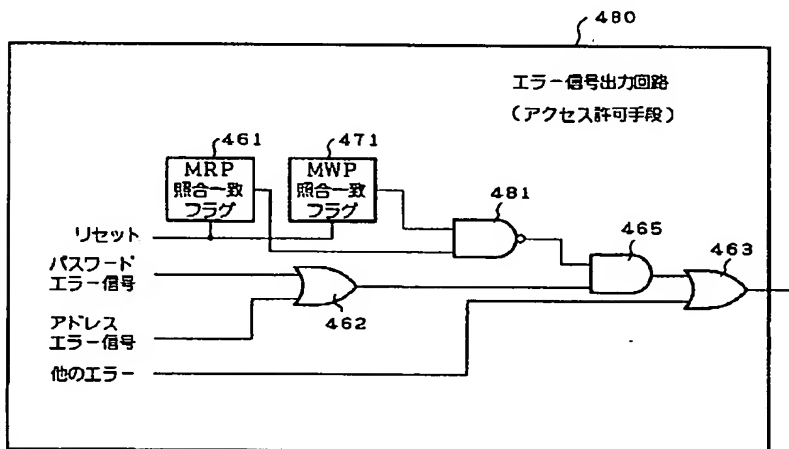


【図22】

リード・ライト装置 非接触式ICカード

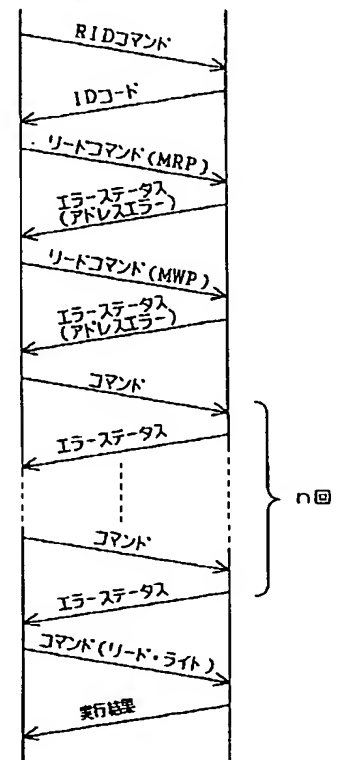


【図21】



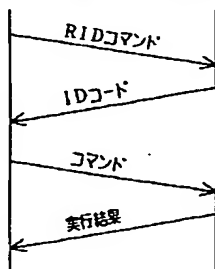
【図24】

リード・ライト装置 非接触式ICカード

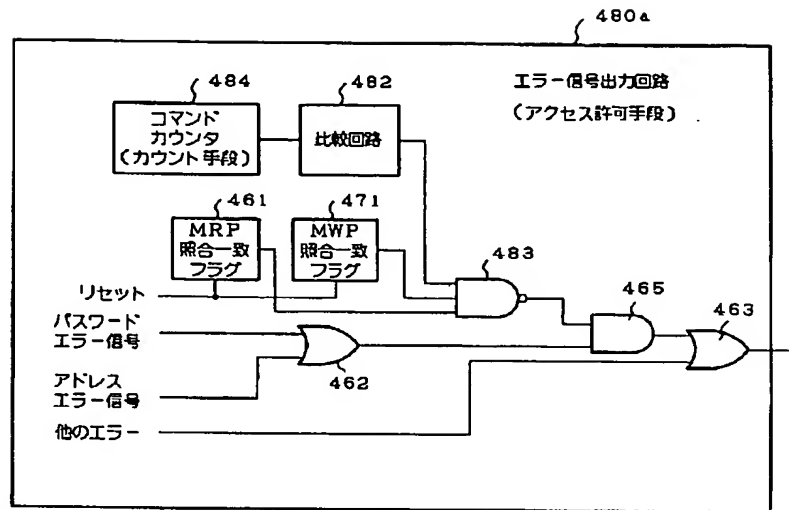


【図27】

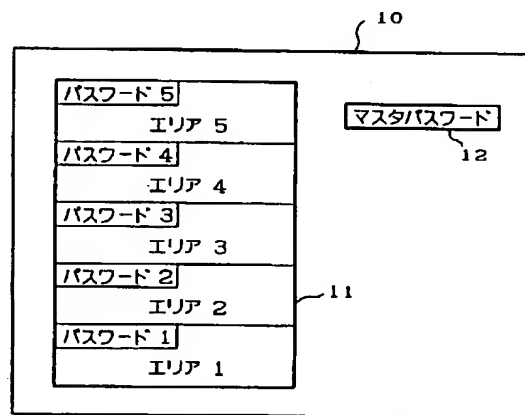
リード・ライト装置 非接触式ICカード



【図23】



【図25】



フロントページの続き

(51) Int. Cl.⁶

H04L 9/32

識別記号

片内整理番号

FI

H04L 9/00

技術表示箇所

673A

673E